

INITIAL SECURITY BRIEFING AND CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT BRIEFING

On file OSD release instructions apply.

I N D E X

Information Security Briefing - - - - -	-TAB A
Security Marking - - - - -	TAB B
Safeguarding of Classified Defense Information - - - -	TAB C
Sections 641, 793, 794, 798, and 952 of Title 18, USC -	TAB D
Section 783(b) of Title 50 - - - - -	TAB E
Intelligence Identities Protection Act of 1982 - - - -	TAB F
Executive Order 12356 - - - - -	-TAB G
Classified Information Nondisclosure Agreement(SF189) -	TAB H

On file OSD release instructions apply.

This briefing was prepared for DoD Personnel under Executive Order 12356. The DoD cannot disclose classified information to Congress unless the information is given "equivalent protection". Since the Congress does not have a general program for information security, this briefing will assist you in properly protecting classified information provided by the DoD.

INFORMATION SECURITY BRIEFING

Welcome to this briefing on the government's information security program. It has been designed to provide an overview of the program and the part that each of us plays in making it work.

This briefing is unclassified.

National Security Information. What is it? Who controls it? How does the system function? We have long recognized the need to protect national security information. Since World War II, we have done so through a series of Executive Orders. On April 2, 1982, the President signed Executive Order 12356. This Order, effective August 1, 1982, provides the framework for our information security program and prescribes a uniform system for classifying, declassifying, and safeguarding national security information.

In signing the Executive Order, the President emphasized that its major purpose is to enhance protection for national security information without permitting excessive classification. To understand the program established under the Order, we must answer some basic questions: For example, what is national security information? National security information is official information that relates to our national defense or foreign relations. Of course not all information concerning our national defense or foreign relations is classified, only that which requires protection in the interests of national security. The act of imposing the Order's protection upon information is called "classification," so we also refer to national security information as classified information.

In what ways may we classify information? Information may be classified in one of two ways--originally or derivatively. Original classification is an initial determination that information requires protection against unauthorized disclosure in the interest of national security. This process includes both the determination of the need to protect the information and the placement of markings to identify the information as classified. Derivative classification is just as its name implies--classification derived from another source. It is the act of incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the markings of the source information.

Let's examine the original and derivative classification processes separately. First, the original classification process. Who may classify information originally? Information may be classified originally only by officials authorized in writing to do so, either by the President or by an official delegated that authority by the President. No one has a right to classify information solely by virtue of rank or position. Although hundreds of thousands of persons are cleared for access to classified information, there are only about 7,000 officials in the entire executive branch who may classify information originally.

What steps must we follow in this process? Before information may be classified originally, it must meet the following tests:

First, the information may only be classified by an executive branch official with original classification authority.

Second, the Government must own, have a proprietary interest in, or otherwise control the information. Control pertains to the government's ability to regulate access to the information.

Third, the authorized classifier must determine that the information falls within one or more of the following classification categories:

Military plans, weapons, or operations; the vulnerabilities or capabilities of systems, installations, projects, or plans relating to national security; foreign government information; intelligence activities (including special activities) or intelligence sources or methods; foreign relations or foreign activities of the United States; scientific, technological, or economic matters relating to the national security; United States Government programs for safeguarding nuclear materials or facilities; cryptology; a confidential source; or other categories of information that require protection in the interest of national security as determined by the President, or other authorized officials.

Fourth, and most importantly, the original classifier must determine that unauthorized disclosure of the information reasonably could be expected to cause damage to the national security.

Are there different levels of classification? Depending upon its sensitivity, we classify information at one of three levels: CONFIDENTIAL - for information whose unauthorized disclosure could reasonably be expected to cause damage to the national security. SECRET - serious damage to the national security, and TOP SECRET - exceptionally grave damage to the national security. We may not use other designations, such as "Administratively Confidential" or "Limited Official Use," to identify national security information. Nor may we combine one of the three authorized designations with any other term - for example, "Top Secret Sensitive". In addition, information under the government's control that is not national security information should not be marked "Top Secret", "Secret" or "Confidential."

Are there any additional prohibitions? The Executive order specifically states that information shall not be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

We have been describing the original classification process. Now let's turn our attention to the derivative classification process. Remember, derivative classification is the act of incorporating, paraphrasing, restating or generating in new form classified source information. Who may derivatively classify? Only those executive branch or contractor employees with the appropriate security clearance, who are required by their work to restate classified source information, may classify derivatively.

How do we classify derivatively? We classify information in one of two ways -- through the use of a source document, usually correspondence or publications generated by an original classification authority; or through the use of a

classification guide. A classification guide is an instruction issued by an original classification authority. For example, the Air Force would issue a classification guide to the contractor producing a missile that includes classified components. The guide instructs the contractor on the elements of information to be classified, the level of classification and its duration. We should check with our security manager on the availability of classification guides that pertain to our programs.

We have now discussed the two ways of classifying information; however, whether classifying originally or derivatively, we may find ourselves in a situation of uncertainty-never classify arbitrarily; when in doubt, find out, from an individual or agency with subject matter expertise.

Now let's examine the markings necessary to place recipients on alert about the sensitivity of classified information. At a minimum, classified documents must indicate the highest classification level of the information; the identity of the original classification authority; the agency or office of origin; and a date or event for declassification, or the standard notation "Originating Agency's Determination Required," sometimes abbreviated "OADR." This marking denotes that at the time of original classification, the classifier is unable to determine a date or event for declassification. In addition, we must mark all portions of a classified document to indicate the level of classification, unless this requirement has been waived.

How do we portion mark a document? We mark each portion of document, including subjects and titles, by placing a parenthetical designation immediately preceding or following the text to which it applies. A portion ordinarily equals a paragraph. There are other marking requirements prescribed by the Order, its implementing directives, and agency regulations. If our job requires familiarity with these markings, we must check with our security manager for information concerning them.

Up to this point we have been talking about the process of classification. Now let's look at the process of declassification. Who may declassify information? Information may be declassified by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the agency head or senior agency official.

How is information declassified? There are several actions that may result in the declassification of information.

First, when it can be determined, the original classifier sets a specific date or event for declassification; when that date or event occurs, the information is automatically declassified.

Second, at any time a citizen may request that information be reviewed for declassification. This is called "mandatory review."

Third, the Archivist of the United States reviews for declassification the permanently valuable records in the National Archives. This is called systematic review for declassification and results in the declassification of millions of pages of formerly classified information. Other agencies may also conduct a systematic review program.

Now that we've looked at the classification and declassification processes, let's examine the subject of safeguarding national security information. What is safeguarding? Safeguarding encompasses a variety of actions specially designed to protect national security information. These include the use, storage, reproduction, transmission, and destruction of classified material under conditions that provide protection and prevent access by unauthorized persons.

Our security manager is the expert we should consult on these actions; however, here are a few basic principles to keep in mind:

To have access, a person must have an appropriate security clearance and a "need-to-know" the information in connection with official duties. Before granting access, the person who controls the information must verify the identity, the security clearance, and the need-to-know of the recipient.

Never perform classified work or hold classified discussions in a non-secure area such as a home, restaurant, car pool, or plane.

Never discuss classified information on the telephone unless using an approved security communications system. While most people recognize the dangers of using the telephone for this purpose, some believe that by using code words, acronyms, or double talk, they somehow render a classified conversation harmless. Don't be misled. Classified information may only be discussed in person or over secure circuits. Most leaks of classified information result from conversations or interviews, not from the compromise of documents. Be especially cautious in dealings with persons not authorized to have access to classified material. It is remarkable how much information appears in the press which can be traced to persons who speak irresponsibly in conversations and interviews.

What other steps do we take to safeguard classified information? Avoid needless exposure of classified material. Lock it up in approved containers, except when needed for working purposes. Memorize safe combinations. Never write the combination on calendars or desk blotters, store it in a desk drawer, or carry it in wallets or purses. Classified information is not personal property and may not be removed from an activity without specific authorization. Upon our transfer or separation, we must return all classified information for which we are responsible to our supervisor or security manager. Destroy all classified information that is no longer required for operational or record purposes. We must check with our security manager for the approved method of destruction. By following these rules and precautions we minimize the threat of unauthorized disclosure. Remember, we expose ourselves to serious penalties if we purposely or even negligently compromise national security information. We must immediately report any actual or suspected unauthorized compromise or disclosure of classified information to our security manager -- we should not try to handle it ourselves. Nor must we hesitate to report incidents for which we may be partially or fully responsible. Our failure to report them is far more likely to result in serious consequences. We hope we have provided some basic answers about our information security program -- any questions should be directed to the security manager. He or she is the professional trained to assist in all these areas. Assistance is also available from the Information Security Oversight Office. The office, which produced this briefing, oversees the information security program throughout the executive branch.

B

MARKING

Executive Order 12356 requires that national security information be marked to place recipients on alert about its sensitivity.

Let's review what we've already learned about classifying national security information. National security information is official information that requires protection against unauthorized disclosure, in the interests of our national defense or foreign policy. We also refer to it as classified information. Executive Order 12356 prescribes three classification levels:

Confidential: For information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

Secret: Serious damage to the national security; and

Top Secret: Exceptional grave damage to the national security;

Information is classified in one of two ways - an original classification decision or a derivative classification decision. Only individuals specifically authorized in writing may classify documents originally. Only cleared personnel who are required by their jobs to restate classified source information may classify derivatively. The classifier - the person who determines that information must be classified, is responsible for assuring that it is properly marked. While the actual markings may be applied by an assistant, the classifier is primarily responsible for their application and accuracy.

With these facts in mind, let's examine the correct procedures to follow in marking classified information. A classified document that an original classifier has determined requires protection under Executive Order 12356 contains the essential markings required under the Order, including portion markings, overall classification markings, the identity of the classifier and a date for declassification.

Let's retrace the steps that the classifier has to follow to mark the document properly. Our first step is to identify the classification level of each portion. A portion is ordinarily defined as a paragraph. Only in this way can the overall classification level be determined. The classifier determines which portion contains no information the unauthorized disclosure of which would damage the national security; therefore, we mark it with the abbreviation (U), for unclassified, in parentheses. Note that the classification designation is placed at the beginning of the portion; some agencies prefer the parenthetical designation at the end of the portion. Either method is permissible under Executive Order 12356. If the classifier determines that a paragraph contains information the unauthorized disclosure of which would cause serious damage to the national security and, therefore, is classified at the Secret level. It's marked with a (S) for Secret. We mark paragraphs, which contain information the unauthorized disclosure of which would cause damage to the national security, with a (C) for Confidential. We also mark the subject or title, if applicable.

Now that we know the classification level of each portion, we have all the elements necessary to determine the overall classification of the document. The overall classification is the highest classification level of information contained in the document. In this case the highest classification is Secret. Therefore, we conspicuously place the word Secret at the top and bottom of the document. If our document contains more than one page, we place the overall marking at the top and bottom of the outside of the front cover, on the title page, on the first page, and on the outside of the back cover. We mark other internal pages either with the overall marking or with a marking indicating the highest classification level of information contained on that page.

The next required marking is called the "classified by" line. It identifies the original classification authority. If that authority is also the person whose name appears as the approving or signing official, it may be omitted. Normally, the identification of the originating agency or office is apparent on the face of the document; if it is not, we place it below the "classified by" line. The last essential marking indicates the duration of classification. When possible the classifier links the duration of classification to a specific date or event. For example, the classifier has determined that its sensitivity will cease on October 12, 1990; the classifier has determined that the information is to be declassified upon a specific event. If the date or event for declassification cannot be determined at the time of classification, the classifier enters the standard notation "Originating Agency's Determination Required," or its abbreviation "OADR," on the "declassify on" line. This indicates that the information must be reviewed by the originator before any declassification action is taken. Occasionally, the changing sensitivity of information enables us to lower its classification level upon a certain date or event. This is known as downgrading. The classifier determines that a document may be downgraded to Secret on July 1, 1988, as an example.

Let's turn now to the marking of derivatively classified documents. From our earlier discussion we learned that a document could be derivatively classified in one of two ways--through the use of a source document or in accordance with instructions in a classification guide. When using a classified source document as the basis for classification, the essential marking elements are carried forward from the source document to our derivative document. For example, A properly marked source document classified by an original classification authority contains all the essential markings--portion marking, overall marking, a "classified by" line, and a "declassify on" line.

Our task is to create a new document that incorporates information from the second paragraph of the source document, a paragraph marked "Secret." In our derivative document no other information is classified. Therefore, we mark it to indicate that the first paragraph, which incorporates the source information, requires protection at the "Secret" level. All other portions, including the title, are marked "(U)" to show that they are unclassified. Looking at all our portion markings, we determine that the highest classification of information is "Secret". We apply that marking as the overall classification. We then refer to the source document to determine the identity of the original classifier, and enter this information on the "classified by" line of our derivative document. Finally, we transfer the declassification instructions from the source document to the "declassify on" line of our derivative document. In this way we achieve consistency in the declassification of like information.

There may be instances in which we use more than one classified source document in creating a derivative document. In these cases the marking procedures are essentially the same. The information incorporated in our derivative document is portion marked at the level indicated in the source documents. We then determine the highest classification of information in any of our portions and apply it as our overall classification level. For our "Classified by" line, we enter the standard notation "multiple sources" to indicate that we are using more than one source. In "multiple source" situations, it is our responsibility as derivative classifiers to maintain the identification of all the classified sources with the file or record of our derivative document. This permits us to retrieve this information when the need arises.

To obtain the entry for our "declassify on" line, we examine the source documents and determine which declassification instruction results in the longest period of protection for the information. For example, here are the declassification instructions on the two source documents used to prepare our derivative document. The first indicates that the information is to be declassified on June 12, 1986. The second requires that the originator review the information prior to its declassification. Since, the second source document would ordinarily result in the longer period of protection, we mark our "declassify on" line "OADR".

The second method of creating a derivative document is through the use of a classification guide. A guide is a document issued by an original classification authority that provides derivative classification instructions. Note that it describes the elements of information that must be protected, the level of protection, and the declassification instructions.

In addition to the essential markings, there may be information contained in a document that requires special markings. For example, a document that contains classified intelligence information. In addition to the essential markings, we apply a warning notice indicating that intelligence sources or methods are involved. We sometimes abbreviate this marking. A document that contains classified information received from a foreign government will indicate the foreign origin of this document by applying the marking "Foreign Government Information," abbreviated "FGI," or some other marking that denotes foreign origin. Sometimes, the fact of foreign origin requires concealment in which case this additional marking is omitted. You may encounter documents Restricted Data or Formerly Restricted Data as defined by the Atomic Energy Act of 1954. In these instances, check with your Security Manager to determine the specific markings to be applied.

Electrically transmitted messages have markings similar to those on paper documents. Frequently, these are abbreviations. Here are a few examples:

For information to be declassified on a specific date: DECL followed by the date.

For information which requires the originating agency's determination prior to declassification action: DECL: OADR.

For information to be automatically downgraded on a specific date or event: DNG followed by the level and date or event.

This has been an overview of the basic marking requirements of Executive Order 12356. Additional information is available in the Information Security Oversight Office Directive No. 1, agency implementing regulations and from the agency Security Manager, the professional trained to assist in all areas of information security management.

C

SAFEGUARDING

Executive Order 12356 requires that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. We safeguard national security information to achieve this goal.

Safeguarding encompasses a variety of activities. These include the storage, control, access, transmission, reproduction and destruction of classified material. Let's begin with storage.

A Top Secret document. How did we store it? We store Top Secret information in an approved security container; in a vault protected by an alarm system and response force; or in any other type of storage facility that provides comparable standards.

Secret and Confidential documents. We store them in the same manner we described for Top Secret information; in a security container that meets the standards set forth in the Information Security Oversight Office Directive No. 1; or a vault or alarmed area authorized by agency regulations.

Storing classified documents in an approved container is not enough. We must also follow certain rules regarding combination locks and padlocks. For example, we must change combinations:

- when placed in use;

- at least once a year regardless of circumstances;

- when a person knowing the combination leaves or no longer requires access;

- when the combination has been subjected to possible compromise; or

- when containers are taken out of service. In these cases, built-in combination locks should be reset to the standard combination of 50-25-50; and padlocks should be reset to 10-20-30.

Only persons with the appropriate security clearance and the necessary expertise may change the combinations.

We also must protect the records of combinations. We classify them at the highest level of information stored in the containers. For this reason, combinations must be memorized. Never write them on calendars or desk blotters, store them in desk drawers, or carry them in wallets or purses.

We next turn to the question of control. When we have possession of classified material we are responsible for:

- protecting it from persons not authorized access to the information;
- securing it in approved containers when not in use, and meeting accountability requirements prescribed by agency regulations.

For Top Secret information, control officers and alternates must be appointed and are responsible for receiving, dispatching and inventorying the information, and for maintaining accountability registers. Agency regulations set forth specific instructions concerning Top Secret, Secret and Confidential accountability requirements. We must become familiar with these instructions.

We have discussed storage and control of classified information, but what about access? We never provide or discuss classified information until we have verified the recipient's need-to-know. Need-to-know is the term we use to indicate that a person requires access to the requested information in connection with official duties.

We now turn to the procedures for transmitting classified documents. Before transmittal, we must: Enclose the classified material in two opaque sealed envelopes or similar wrappings. Place the address of the recipient, the overall classification, and any special markings or instructions on the inner envelope. Attach a classified document receipt to the inner envelope if it contains Top Secret or Secret material. Agency regulations may require document receipts for Confidential material as well. Place the name and address of the recipient on the outer envelope as well as the return address of the sender. Never place classification marking on the outer envelope. The material is now ready for transmittal. Transmit Top Secret material only e direct contract with the recipient, by State Department or Armed Forces Courier Systems, or by messenger service approved by agency heads for the transmittal of Top Secret material.

Transmit Secret material by: any of the means approved for Top Secret; U.S. Postal Service registered mail within and between the United States and its territories, or other means set forth in agency regulations.

In addition to the methods for transmitting Top Secret and Secret, agency heads may authorize the transmittal of Confidential material by U.S. Postal Service certified, first class or express mail. Consult agency regulations for the transmission of classified material outside the United States and its territories.

We next consider the reproduction of classified material. Never reproduce classified information unless required by operational considerations and only on approved equipment. As a general rule, Top Secret information may not be reproduced without the consent of the originating agency. The originating agency may also place restrictions on the reproduction of Secret or Confidential material.

Like other federal records, we dispose of classified information when it is no longer needed for operational or reference purposes. Frequently this requires its destruction. Destroy classified material by one of the following approved means: burning, pulping, pulverizing, shredding, or other mutilation sufficient to preclude recognition or reconstruction of the information. Also destroy other classified waste, such as handwritten notes, carbon paper, typewriter ribbons and working papers.

Agency regulations may also require the maintenance of records of destruction. Before we end our discussion of safeguarding classified information, let's examine some special issues.

The first issue concerns the compromise of classified information. By taking a few precautions we can minimize this treat. For example:

- Avoid needless exposure of classified information;

- Lock it up in approved containers when not in use;

- Never discuss classified information on the telephone except over secured circuits;

- memorize safe combinations;

- Upon transfer or separation, return all classified information to our supervisor or security manager;

- Ensure that persons attending classified meetings possess the appropriate security clearance and need-to-know, and that any notes, working papers, minutes or summaries of the meeting are properly safeguarded; and

- Report all suspected compromise or unauthorized disclosure of national security information to the security manager.

Another concern is leaks. Most leaks of classified information result from conversations or interviews, not from the compromise of documents. We must be especially cautious in our dealings with persons not authorized to have access to classified information. Remember, some reporters and other media representatives routinely seek out this information from unwitting or irresponsible individuals and publish it. The burden of preventing these leaks rests entirely on us.

This has been an overview of the basic safeguarding requirements of Executive Order 12356. Additional information is available in the Information Security Oversight Office Directive No. 1, agency implementing regulations and from the agency security manager, the professional trained to assist in all areas of information security management.

D

EMBEZZLEMENT AND THEFT

Excerpts from Title 18, USC

§ 641. Public money, property or records

Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted.

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of \$100, he shall be fined not more than \$1,000 or imprisoned not more than one year, or both.

The word "value" means face, par or market value, or cost price, either wholesale or retail, whichever is greater.

Excerpts from Title 18, USC

Section 793. Gathering, Transmitting, or Losing Defense Information

(a) Whoever, for the purposes of obtaining information respecting the national defense with intent or reason to believe that the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling, station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter (section 792 et seq. of this title); or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retracts the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer.

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy. (June 25, 1948, c. 645, section 1, 62 Stat. 736; Sept. 23, 1950, c. 1024, Title I, section 18, 64 Stat. 1003.)

Excerpts from Title 18, USC

Section 794. Gathering or Delivering Defense Information to Aid Foreign Government.

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.

(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy. (June 25, 1948, c. 645, section 1, 62 Stat. 737; Sept. 3, 1954, c. 1261, Title II, section 201, 68 Stat. 1219.)

Excerpts from Title 18, USC

Section 798 (799). Temporary Extension of Section 794.

The provisions of section 794 of this title, as amended and extended by section 1(a)(29) of the Emergency Powers Continuation Act (66 Stat. 333), as further amended by Public Law 12, Eighty-third Congress, in addition to coming into full force and effect in time of war shall remain in full force and effect until six months after the termination of the national emergency proclaimed by the President on December 16, 1950 (Proc. 2912, 3 C.F.R., 1950 Sup., p. 71), or such earlier date as may be prescribed by concurrent resolution of the Congress, and acts which would give rise to legal consequences and penalties under section 794 when performed during a state of war shall give rise to the same legal consequences and penalties when they are performed during the period above provided for. (June 30, 1953, c. 175, section 4, 67 Stat. 133.)

Excerpts from Title 18, USC

§ 952. Diplomatic codes and correspondence

Whoever, by virtue of his employment by the United States, obtains from another or has or has had custody of or access to, any official diplomatic code or any matter prepared in any such code, or which purports to have been prepared in any such code, or which purports to have been prepared in any such code, and without authorization or competent authority, willfully publishes or furnishes to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

E

LEVEL 1 - 13 OF 24 SUBSECTIONS

TITLE 50. - WAR AND NATIONAL DEFENSE

§ 783. Offenses.

SEP 23, 1950

§§ 783. (b) Communication of classified information by Government officer or employee

It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to be an agent or representative of any foreign government or an officer or member of any Communist organization as defined in paragraph (5) of section 782 of this title, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President, or by the head of the department, agency, or corporation by which this officer or employee is employed, to make such disclosure of such information.

F

PUBLIC LAW 97-200—JUNE 23, 1982

**INTELLIGENCE IDENTITIES PROTECTION
ACT OF 1982**

96 STAT. 122

PUBLIC LAW 97-200—JUNE 23, 1982

Public Law 97-200
97th Congress

An Act

June 23, 1982
[H.R. 4]

To amend the National Security Act of 1947 to prohibit the unauthorized disclosure of information identifying certain United States intelligence officers, agents, informants, and sources.

Intelligence
Identities
Protection Act
of 1982.
50 USC 401 note.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Intelligence Identities Protection Act of 1982".

SEC. 2. (a) The National Security Act of 1947 is amended by adding at the end thereof the following new title:

"TITLE VI—PROTECTION OF CERTAIN NATIONAL SECURITY
INFORMATION

"PROTECTION OF IDENTITIES OF CERTAIN UNITED STATES UNDERCOVER
INTELLIGENCE OFFICERS, AGENTS, INFORMANTS, AND SOURCES

50 USC 421.

"SEC. 601. (a) Whoever, having or having had authorized access to classified information that identifies a covert agent, intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined not more than \$50,000 or imprisoned not more than ten years, or both.

"(b) Whoever, as a result of having authorized access to classified information, learns the identity of a covert agent and intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined not more than \$25,000 or imprisoned not more than five years, or both.

"(c) Whoever, in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, discloses any information that identifies an individual as a covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such individual and that the United States is taking affirmative measures to conceal such individual's classified intelligence relationship to the United States, shall be fined not more than \$15,000 or imprisoned not more than three years, or both.

"DEFENSES AND EXCEPTIONS

50 USC 422.

"SEC. 602. (a) It is a defense to a prosecution under section 601 that before the commission of the offense with which the defendant

PUBLIC LAW 97-200—JUNE 23, 1982

96 STAT. 123

is charged, the United States had publicly acknowledged or revealed the intelligence relationship to the United States of the individual the disclosure of whose intelligence relationship to the United States is the basis for the prosecution.

“(b)(1) Subject to paragraph (2), no person other than a person committing an offense under section 601 shall be subject to prosecution under such section by virtue of section 2 or 4 of title 18, United States Code, or shall be subject to prosecution for conspiracy to commit an offense under such section.

“(2) Paragraph (1) shall not apply (A) in the case of a person who acted in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, or (B) in the case of a person who has authorized access to classified information.

“(c) It shall not be an offense under section 601 to transmit information described in such section directly to the Select Committee on Intelligence of the Senate or to the Permanent Select Committee on Intelligence of the House of Representatives.

Information,
transmittal to
congressional
committees.

“(d) It shall not be an offense under section 601 for an individual to disclose information that solely identifies himself as a covert agent.

“REPORT

“SEC. 603. (a) The President, after receiving information from the Director of Central Intelligence, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives an annual report on measures to protect the identities of covert agents, and on any other matter relevant to the protection of the identities of covert agents.

50 USC 423.

“(b) The report described in subsection (a) shall be exempt from any requirement for publication or disclosure. The first such report shall be submitted no later than February 1, 1983.

“EXTRATERRITORIAL JURISDICTION

“SEC. 604. There is jurisdiction over an offense under section 601 committed outside the United States if the individual committing the offense is a citizen of the United States or an alien lawfully admitted to the United States for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act).

50 USC 424.

8 USC 1101.

“PROVIDING INFORMATION TO CONGRESS

“SEC. 605. Nothing in this title may be construed as authority to withhold information from the Congress or from a committee of either House of Congress.

50 USC 425.

“DEFINITIONS

“SEC. 606. For the purposes of this title:

50 USC 426.

“(1) The term ‘classified information’ means information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive

96 STAT. 124

PUBLIC LAW 97-200—JUNE 23, 1982

order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security.

“(2) The term ‘authorized’, when used with respect to access to classified information, means having authority, right, or permission pursuant to the provisions of a statute, Executive order, directive of the head of any department or agency engaged in foreign intelligence or counterintelligence activities, order of any United States court, or provisions of any Rule of the House of Representatives or resolution of the Senate which assigns responsibility within the respective House of Congress for the oversight of intelligence activities.

“(3) The term ‘disclose’ means to communicate, provide, impart, transmit, transfer, convey, publish, or otherwise make available.

“(4) The term ‘covert agent’ means—

“(A) an officer or employee of an intelligence agency or a member of the Armed Forces assigned to duty with an intelligence agency—

“(i) whose identity as such an officer, employee, or member is classified information, and

“(ii) who is serving outside the United States or has within the last five years served outside the United States; or

“(B) a United States citizen whose intelligence relationship to the United States is classified information, and—

“(i) who resides and acts outside the United States as an agent of, or informant or source of operational assistance to, an intelligence agency, or

“(ii) who is at the time of the disclosure acting as an agent of, or informant to, the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation; or

“(C) an individual, other than a United States citizen, whose past or present intelligence relationship to the United States is classified information and who is a present or former agent of, or a present or former informant or source of operational assistance to, an intelligence agency.

“(5) The term ‘intelligence agency’ means the Central Intelligence Agency, a foreign intelligence component of the Department of Defense, or the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation.

“(6) The term ‘informant’ means any individual who furnishes information to an intelligence agency in the course of a confidential relationship protecting the identity of such individual from public disclosure.

“(7) The terms ‘officer’ and ‘employee’ have the meanings given such terms by section 2104 and 2105, respectively, of title 5, United States Code.

“(8) The term ‘Armed Forces’ means the Army, Navy, Air Force, Marine Corps, and Coast Guard.

“(9) The term ‘United States’, when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

“(10) The term ‘pattern of activities’ requires a series of acts with a common purpose or objective.”

PUBLIC LAW 97-200—JUNE 23, 1982

96 STAT. 125

(b) The table of contents at the beginning of such Act is amended by adding at the end thereof the following:

"TITLE VI—PROTECTION OF CERTAIN NATIONAL SECURITY INFORMATION

"Sec. 601. Protection of identities of certain United States undercover intelligence officers, agents, informants, and sources.

"Sec. 602. Defenses and exceptions.

"Sec. 603. Report.

"Sec. 604. Extraterritorial jurisdiction.

"Sec. 605. Providing information to Congress.

"Sec. 606. Definitions."

Approved June 23, 1982.

LEGISLATIVE HISTORY—H.R. 4 (S. 391):

HOUSE REPORTS: No. 97-221 (Comm. on Intelligence) and No. 97-580 (Comm. of Conference).

SENATE REPORT No. 97-201 accompanying S. 391 (Comm. on the Judiciary).

CONGRESSIONAL RECORD:

Vol. 127 (1981): Sept. 23, considered and passed House.

Vol. 128 (1982): Feb. 25, Mar. 1, 15-17, S. 391 considered in Senate.

Mar. 18, H.R. 4 considered and passed Senate, amended.

June 2, 3, House considered and agreed to conference report.

June 10, Senate agreed to conference report.

WEEKLY COMPILATION OF PRESIDENTIAL DOCUMENTS, Vol. 18, No. 25 (1982): June 23, Presidential statement.

G

14874

Federal Register

Vol. 47, No. 66

Tuesday, April 6, 1982

Presidential Documents

Title 3—

Executive Order 12356 of April 2, 1982

The President

National Security Information

TABLE OF CONTENTS

	<i>[FR Page]</i>
Preamble	[14874]
<i>Part 1. Original Classification</i>	
1.1 Classification Levels	[14874]
1.2 Classification Authority	[14874]
1.3 Classification Categories	[14875]
1.4 Duration of Classification	[14876]
1.5 Identification and Markings	[14877]
1.6 Limitations on Classification	[14877]
<i>Part 2. Derivative Classification</i>	
2.1 Use of Derivative Classification	[14878]
2.2 Classification Guides	[14878]
<i>Part 3. Declassification and Downgrading</i>	
3.1 Declassification Authority	[14878]
3.2 Transferred Information	[14879]
3.3 Systematic Review for Declassification	[14879]
3.4 Mandatory Review for Declassification	[14879]
<i>Part 4. Safeguarding</i>	
4.1 General Restrictions on Access	[14880]
4.2 Special Access Programs	[14881]
4.3 Access by Historical Researchers and Former Presidential Appointees	[14881]
<i>Part 5. Implementation and Review</i>	
5.1 Policy Direction	[14881]
5.2 Information Security Oversight Office	[14881]
5.3 General Responsibilities	[14882]
5.4 Sanctions	[14882]
<i>Part 6. General Provisions</i>	
6.1 Definitions	[14883]
6.2 General	[14883]

This Order prescribes a uniform system for classifying, declassifying, and safeguarding national security information. It recognizes that it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Information may not be classified under this Order unless its disclosure reasonably could be expected to cause damage to the national security.

NOW, by the authority vested in me as President by the Constitution and laws of the United States of America, it is hereby ordered as follows:

Part 1

Original Classification

Section 1.1 *Classification Levels.*

(a) National security information (hereinafter "classified information") shall be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(b) Except as otherwise provided by statute, no other terms shall be used to identify classified information.

(c) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.

Sec. 1.2 Classification Authority.

(a) *Top Secret*. The authority to classify information originally as Top Secret may be exercised only by:

- (1) the President;
- (2) agency heads and officials designated by the President in the Federal Register; and
- (3) officials delegated this authority pursuant to Section 1.2(d).

(b) *Secret*. The authority to classify information originally as Secret may be exercised only by:

- (1) agency heads and officials designated by the President in the Federal Register;
- (2) officials with original Top Secret classification authority; and
- (3) officials delegated such authority pursuant to Section 1.2(d).

(c) *Confidential*. The authority to classify information originally as Confidential may be exercised only by:

- (1) agency heads and officials designated by the President in the Federal Register;
- (2) officials with original Top Secret or Secret classification authority; and
- (3) officials delegated such authority pursuant to Section 1.2(d).

(d) Delegation of Original Classification Authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this Order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) Original Top Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Section 1.2(a)(2); and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original Top Secret classification authority by the agency head.

(3) Original Secret classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2) and 1.2(b)(1); an official with original Top Secret classification authority; and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original Secret classification authority by the agency head.

(4) Original Confidential classification authority may be delegated only by the President; an agency head or official designated pursuant to Sections 1.2(a)(2), 1.2(b)(1) and 1.2(c)(1); an official with original Top Secret classification author-

ity; and the senior official designated under Section 5.3(a)(1), provided that official has been delegated original classification authority by the agency head.

(5) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this Order. It shall identify the official delegated the authority by name or position title. Delegated classification authority includes the authority to classify information at the level granted and lower levels of classification.

(e) *Exceptional Cases.* When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Sec. 1.3 *Classification Categories.*

(a) Information shall be considered for classification if it concerns:

- (1) military plans, weapons, or operations;
- (2) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;
- (3) foreign government information;
- (4) intelligence activities (including special activities), or intelligence sources or methods;
- (5) foreign relations or foreign activities of the United States;
- (6) scientific, technological, or economic matters relating to the national security;
- (7) United States Government programs for safeguarding nuclear materials or facilities;
- (8) cryptology;
- (9) a confidential source; or
- (10) other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been delegated original classification authority by the President. Any determination made under this subsection shall be reported promptly to the Director of the Information Security Oversight Office.

(b) Information that is determined to concern one or more of the categories in Section 1.3(a) shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

(c) Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

(d) Information classified in accordance with Section 1.3 shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

Sec. 1.4 Duration of Classification.

(a) Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.

(b) Automatic declassification determinations under predecessor orders shall remain valid unless the classification is extended by an authorized official of the originating agency. These extensions may be by individual documents or categories of information. The agency shall be responsible for notifying holders of the information of such extensions.

(c) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of this Order.

Sec. 1.5 Identification and Markings.

(a) At the time of original classification, the following information shall be shown on the face of all classified documents, or clearly associated with other forms of classified information in a manner appropriate to the medium involved, unless this information itself would reveal a confidential source or relationship not otherwise evident in the document or information:

- (1) one of the three classification levels defined in Section 1.1;
- (2) the identity of the original classification authority if other than the person whose name appears as the approving or signing official;
- (3) the agency and office of origin; and
- (4) the date or event for declassification, or the notation "Originating Agency's Determination Required."

(b) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified. Agency heads may, for good cause, grant and revoke waivers of this requirement for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

(c) Marking designations implementing the provisions of this Order, including abbreviations, shall conform to the standards prescribed in implementing directives issued by the Information Security Oversight Office.

(d) Foreign government information shall either retain its original classification or be assigned a United States classification that shall ensure a degree of protection at least equivalent to that required by the entity that furnished the information.

(e) Information assigned a level of classification under predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Omitted markings may be inserted on a document by the officials specified in Section 3.1(b).

Sec. 1.6 Limitations on Classification.

(a) In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) The President or an agency head or official designated under Sections 1.2(a)(2), 1.2(b)(1), or 1.2(c)(1) may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information

may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office.

(d) Information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of this Order (Section 3.4) if such classification meets the requirements of this Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior agency official designated under Section 5.3(a)(1), or an official with original Top Secret classification authority.

Part 2

Derivative Classification

Sec. 2.1 Use of Derivative Classification.

(a) Derivative classification is (1) the determination that information is in substance the same as information currently classified, and (2) the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

- (1) observe and respect original classification decisions; and
- (2) carry forward to any newly created documents any assigned authorized markings. The declassification date or event that provides the longest period of classification shall be used for documents classified on the basis of multiple sources.

Sec. 2.2 Classification Guides.

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information.

(b) Each guide shall be approved personally and in writing by an official who:

- (1) has program or supervisory responsibility over the information or is the senior agency official designated under Section 5.3(a)(1); and
- (2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agency heads may, for good cause, grant and revoke waivers of the requirement to prepare classification guides for specified classes of documents or information. The Director of the Information Security Oversight Office shall be notified of any waivers.

Part 3

Declassification and Downgrading

Sec. 3.1 Declassification Authority.

(a) Information shall be declassified or downgraded as soon as national security considerations permit. Agencies shall coordinate their review of classified information with other agencies that have a direct interest in the subject matter. Information that continues to meet the classification requirements prescribed by Section 1.3 despite the passage of time will continue to be protected in accordance with this Order.

(b) Information shall be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same position; the originator's successor; a supervisory official of either; or officials delegated such authority in writing by the agency head or the senior agency official designated pursuant to Section 5.3(a)(1).

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this Order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the National Security Council. The information shall remain classified, pending a prompt decision on the appeal.

(d) The provisions of this Section shall also apply to agencies that, under the terms of this Order, do not have original classification authority, but that had such authority under predecessor orders.

Sec. 3.2 *Transferred Information.*

(a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this Order.

(b) In the case of classified information that is not officially transferred as described in Section 3.2(a), but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this Order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with this Order, the directives of the Information Security Oversight Office, and agency guidelines.

Sec. 3.3 *Systematic Review for Declassification.*

(a) The Archivist of the United States shall, in accordance with procedures and timeframes prescribed in the Information Security Oversight Office's directives implementing this Order, systematically review for declassification or downgrading (1) classified records accessioned into the National Archives of the United States, and (2) classified presidential papers or records under the Archivist's control. Such information shall be reviewed by the Archivist for declassification or downgrading in accordance with systematic review guidelines that shall be provided by the head of the agency that originated the information, or in the case of foreign government information, by the Director of the Information Security Oversight Office in consultation with interested agency heads.

(b) Agency heads may conduct internal systematic review programs for classified information originated by their agencies contained in records determined by the Archivist to be permanently valuable but that have not been accessioned into the National Archives of the United States.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

Sec. 3.4. *Mandatory Review for Declassification.*

(a) Except as provided in Section 3.4(b), all information classified under this Order or predecessor orders shall be subject to a review for declassification by the originating agency, if:

(1) the request is made by a United States citizen or permanent resident alien, a federal agency, or a State or local government; and

(2) the request describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort.

(b) Information originated by a President, the White House Staff, by committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempted from the provisions of Section 3.4(a). The Archivist of the United States shall have the authority to review, downgrade and declassify information under the control of the Administrator of General Services or the Archivist pursuant to sections 2107, 2107 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Any decision by the Archivist may be appealed to the Director of the Information Security Oversight Office. Agencies with primary subject matter interest shall be notified promptly of the Director's decision on such appeals and may further appeal to the National Security Council. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information no longer requiring protection under this Order. They shall release this information unless withholding is otherwise authorized under applicable law.

(d) Agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They shall also provide a means for administratively appealing a denial of a mandatory review request.

(e) The Secretary of Defense shall develop special procedures for the review of cryptologic information, and the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, after consultation with affected agencies. The Archivist shall develop special procedures for the review of information accessioned into the National Archives of the United States.

(f) In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this Order:

(1) An agency shall refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classifiable under this Order.

(2) When an agency receives any request for documents in its custody that were classified by another agency, it shall refer copies of the request and the requested documents to the originating agency for processing, and may, after consultation with the originating agency, inform the requester of the referral. In cases in which the originating agency determines in writing that a response under Section 3.4(f)(1) is required, the referring agency shall respond to the requester in accordance with that Section.

Part 4

Safeguarding

Sec. 4.1 *General Restrictions on Access.*

(a) A person is eligible for access to classified information provided that a determination of trustworthiness has been made by agency heads or designated officials and provided that such access is essential to the accomplishment of lawful and authorized Government purposes.

(b) Controls shall be established by each agency to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed only under conditions that will provide adequate protection and prevent access by unauthorized persons.

(c) Classified information shall not be disseminated outside the executive branch except under conditions that ensure that the information will be given protection equivalent to that afforded within the executive branch.

(d) Except as provided by directives issued by the President through the National Security Council, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. For purposes of this Section, the Department of Defense shall be considered one agency.

Sec. 4.2 Special Access Programs.

(a) Agency heads designated pursuant to Section 1.2(a) may create special access programs to control access, distribution, and protection of particularly sensitive information classified pursuant to this Order or predecessor orders. Such programs may be created or continued only at the written direction of these agency heads. For special access programs pertaining to intelligence activities (including special activities but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence.

(b) Each agency head shall establish and maintain a system of accounting for special access programs. The Director of the Information Security Oversight Office, consistent with the provisions of Section 5.2(b)(4), shall have non-delegable access to all such accountings.

Sec. 4.3 Access by Historical Researchers and Former Presidential Appointees.

(a) The requirement in Section 4.1(a) that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived as provided in Section 4.3(b) for persons who:

- (1) are engaged in historical research projects, or
- (2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under Section 4.3(a) may be granted only if the originating agency:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this Order; and

(3) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.

Part 5

Implementation and Review

Sec. 5.1 Policy Direction.

(a) The National Security Council shall provide overall policy direction for the information security program.

(b) The Administrator of General Services shall be responsible for implementing and monitoring the program established pursuant to this Order. The Administrator shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

Sec. 5.2 Information Security Oversight Office.

(a) The Information Security Oversight Office shall have a full-time Director appointed by the Administrator of General Services subject to approval by the President. The Director shall have the authority to appoint a staff for the Office.

(b) The Director shall:

- (1) develop, in consultation with the agencies, and promulgate, subject to the approval of the National Security Council, directives for the implementation of this Order, which shall be binding on the agencies;
- (2) oversee agency actions to ensure compliance with this Order and implementing directives;
- (3) review all agency implementing regulations and agency guidelines for systematic declassification review. The Director shall require any regulation or guideline to be changed if it is not consistent with this Order or implementing directives. Any such decision by the Director may be appealed to the National Security Council. The agency regulation or guideline shall remain in effect pending a prompt decision on the appeal;
- (4) have the authority to conduct on-site reviews of the information security program of each agency that generates or handles classified information and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill the Director's responsibilities. If these reports, inspections, or access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior official designated under Section 5.3(a)(1) may deny access. The Director may appeal denials to the National Security Council. The denial of access shall remain in effect pending a prompt decision on the appeal;
- (5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval;
- (6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program;
- (7) have the authority to prescribe, after consultation with affected agencies, standard forms that will promote the implementation of the information security program;
- (8) report at least annually to the President through the National Security Council on the implementation of this Order; and
- (9) have the authority to convene and chair interagency meetings to discuss matters pertaining to the information security program.

Sec. 5.3 General Responsibilities.

Agencies that originate or handle classified information shall:

- (a) designate a senior agency official to direct and administer its information security program, which shall include an active oversight and security education program to ensure effective implementation of this Order;
- (b) promulgate implementing regulations. Any unclassified regulations that establish agency information security policy shall be published in the Federal Register to the extent that these regulations affect members of the public;
- (c) establish procedures to prevent unnecessary access to classified information, including procedures that (i) require that a demonstrable need for access to classified information is established before initiating administrative clearance procedures, and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs; and
- (d) develop special contingency plans for the protection of classified information used in or near hostile or potentially hostile areas.

Sec. 5.4 Sanctions.

- (a) If the Director of the Information Security Oversight Office finds that a violation of this Order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior official

designated under Section 5.3(a)(1) so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, and grantees shall be subject to appropriate sanctions if they:

(1) knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under this Order or predecessor orders;-

(2) knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive; or

(3) knowingly and willfully violate any other provision of this Order or implementing directive.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) Each agency head or the senior official designated under Section 5.3(a)(1) shall ensure that appropriate and prompt corrective action is taken whenever a violation under Section 5.4(b) occurs. Either shall ensure that the Director of the Information Security Oversight Office is promptly notified whenever a violation under Section 5.4(b) (1) or (2) occurs.

Part 6

General Provisions

Sec. 6.1 *Definitions.*

(a) "Agency" has the meaning provided at 5 U.S.C. 552(e).

(b) "Information" means any information or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(c) "National security information" means information that has been determined pursuant to this Order or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(d) "Foreign government information" means:

(1) information provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

(e) "National security" means the national defense or foreign relations of the United States.

(f) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

(g) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

Sec. 6.2 *General.*

(a) Nothing in this Order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and

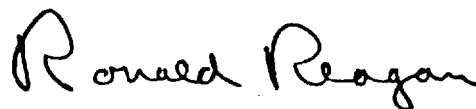
declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this Order with respect to any question arising in the course of its administration.

(c) Nothing in this Order limits the protection afforded any information by other provisions of law.

(d) Executive Order No. 12065 of June 28, 1978, as amended, is revoked as of the effective date of this Order.

(e) This Order shall become effective on August 1, 1982.



THE WHITE HOUSE,
April 2, 1982.

[FR Doc. 82-8320

Filed 4-2-82; 2:52 pm]

Billing code 3195-01-M

Editorial Note: The President's statement of Apr. 2, 1982, on signing Executive Order 12356 is printed in the *Weekly Compilation of Presidential Documents* (vol. 18, no. 13)

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between _____ and the United States
(Name - Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is information that is either classified or classifiable under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.
2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.
3. I have been advised and am aware that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge such information unless I have officially verified that the recipient has been properly authorized by the United States Government to receive it or I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) last granting me a security clearance that such disclosure is permitted. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.
4. I have been advised and am aware that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; and the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised and am aware that any unauthorized disclosure of classified information by me may constitute a violation or violations of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and 952, Title 18, United States Code, the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.
5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.
6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.
7. I understand that all information to which I may obtain access by signing this Agreement is now and will forever remain the property of the United States Government. I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials which have, or may have, come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.
8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.
9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.
10. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, Section 783(b) of Title 50, United States Code, the Intelligence Identities Protection Act of 1982, and Executive Order 12356, so that I may read them at this time, if I so choose.
11. I make this Agreement without mental reservation or purpose of evasion.

SIGNATURE	DATE	SOCIAL SECURITY NO. (See notice below)
ORGANIZATION		

The execution of this Agreement was witnessed by the undersigned, who, on behalf of the United States Government, agreed to its terms and accepted it as a prior condition of authorizing access to classified information.

WITNESS AND ACCEPTANCE:

SIGNATURE	DATE
ORGANIZATION	

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations.